DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

GINL Enterprise Network
Updated April 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Sharing Services
Email : PIA@state.gov

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public?**

YES _X__ NO___

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor".**

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail address: PIA@state.gov.

2) Does a Privacy Act system of records already exist?

YES ___ NO_X_

If yes, please provide the following:
System Name _____ Number ____

If no, a Privacy system of records description will need to be created for this data.

3) What is the purpose of the system/application?

GINL is a General Support System (GSS) used to assist the Bureau for International Narcotics and Law Enforcement Affairs (INL) in supporting two of the Department of State's strategic goals: (1) to reduce the entry of illegal drugs into the United States; and (2) to minimize the impact of international crime on the United States and its citizens.

4) What legal authority authorizes the purchase or development of this system/application?

2008 National Drug Control Strategy

C. DATA IN THE SYSTEM

1) What categories of individuals are covered in the system?

Individual information includes current employees, former employees, prospective employees, and contractors of the U.S. Government and DynCorp International.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

Information is obtained directly from the individual.

b. What type of information is collected from the source of the information?

- Information relating to race, national or ethnic origin, religion, age, marital or family status;
- Information relating to education, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and
- Name, , address, telephone number and e-mail address.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

Information typically is provided by the employer and is verified by the individual's supervisor, the Bureau of Human Resources (HR), security personnel or, in the case of a contractor, an HR vendor called HR Plus.

b. How will data be checked for completeness?

Personnel in HR and security are tasked with assuring completeness of documents pertaining to these types of information. These personnel begin their document checking prior to hiring, and continue through employment and separation of the employee.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Information typically is provided by the employer and is verified by the individual's supervisor, HR, or security personnel. Changes or updates to personally identifiable information (PII) is initiated by the individual to whom the PII belongs .

D. INTENDED USE OF THE DATA

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

All information contained in the GINL system is relevant and necessary to the purpose to which the GSS is designed.

Relevancy: Information is collected for the purpose of training and certification of individuals, employment actions, etc.

2) **Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?**
No.

3) **Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?**
No.

4) **Will the new data be placed in the individual's record?**
Data will be constantly updated by appropriate personnel to ensure individual data is relevant and current.

5) **How will the new data be verified for relevance and accuracy?**
It is dependent on the personnel who are entering the information to determine the relevancy and accuracy of the information. Additionally, a third party HR vendor (HR Plus) will verify the accuracy of some data provided by prospective employees.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**
Information retrieved is dependent on the user requirements and resources available. The use of DB and other retrieval software requires approval by Department of State officials prior to usage.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
Due to the wide range assets available to GINL users within the system, it is difficult to determine all reports that can be generated by users of the system. Certainly, statistical information, HR reports, aircraft maintenance reports, etc. may be produced at any required point.

The reports generated may contain personal identifiable information (PII) to include the following:

- Information relating to race, national or ethnic origin, religion, age, marital or family status;
- Information relating to education, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and
- Name, SSN, address, telephone number and e-mail address.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**
GINL GSS is configured using Department standard configuration and set standards throughout the Enterprise. Because information is maintained by

each user, the proper training and signing of user agreement forms are consistent throughout each site.

2) **What are the retention periods of data in this system?**
PII data is retained in the system for an undetermined amount of time.

A back-up system retains PII for a minimum of 180 days at which time the data is deleted.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
Data disposition is in accordance with Federal guidelines.

GINL is not designed to collect nor retain reports with PII. Ad-hoc reports may contain PII and are not retained on the system.. Users generating such reports and printing them out are directed to protect such information according to applicable laws.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
No, only approved DOS technologies are used on the GINL GSS.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**
The use of technology in this system does not currently impact privacy concerns.

Only authorized individuals are granted access to the GINL network. In order to gain access, the user must submit a user agreement form and obtain approval by the respective manager. This limits the access to only cleared/approved personnel.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**
This system does not provide the capability to identify, locate, or monitor individuals.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**
The system displays a Privacy Act Statement when individuals log onto the system. GINL is not under modification at this time.

Information in GINL is static, therefore, the need to update the Privacy Act System of Records Notice is not required.

8) **Are there forms associated with the system? YES _X_ NO ___**

If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

GINL has the capability to generate forms. Most forms do not collect PII .

GINL utilizes a user agreement form which contains the privacy act statement and users signing this form acknowledge they understand the privacy act statement. Additionally, when users are logging into the GINL network, they are prompted with the user acknowledgement warning banner which cites the privacy act of 1974.

The system does not automatically generate automated markings on information system output. It is dependent upon the user to place appropriate markings and ensure proper protection of such information.

F. ACCESS TO DATA

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**

Data is available to approved Department of State employees, contractors, users, managers, system administrators and developers.

2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Only authorized individuals are granted access to the GINL network. Access requires the user to submit a user agreement form and obtain approval by his or her respective manager. This limits the access to only cleared/approved personnel with a "need-to-know" role and utilization of "least privilege".

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

User access is restricted to a "need-to-know" basis and utilization of "least privilege." This is accomplished by using access control lists and active directory.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**

GINL GSS does not currently audit authorized users accessing data for which they have network privileges and/or permissions.

Upon a user given access to any system, the user/system administrator is required to sign a user agreement form which dictates policy and procedures regarding proper usage of the network.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Contractor personnel do have design and development access to the system. Each user is approved by the Department of State prior to gaining access, which includes submission of a user agreement form referencing the Privacy Act of 1974.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

GINL GSS which houses other major applications utilizes the GINL backbone. Currently, there are no major application interfaces with the ability to interface with GINL servers and/or workstations.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?** No.

8) **Who is responsible for assuring proper use of the SHARED data?**
N/A.